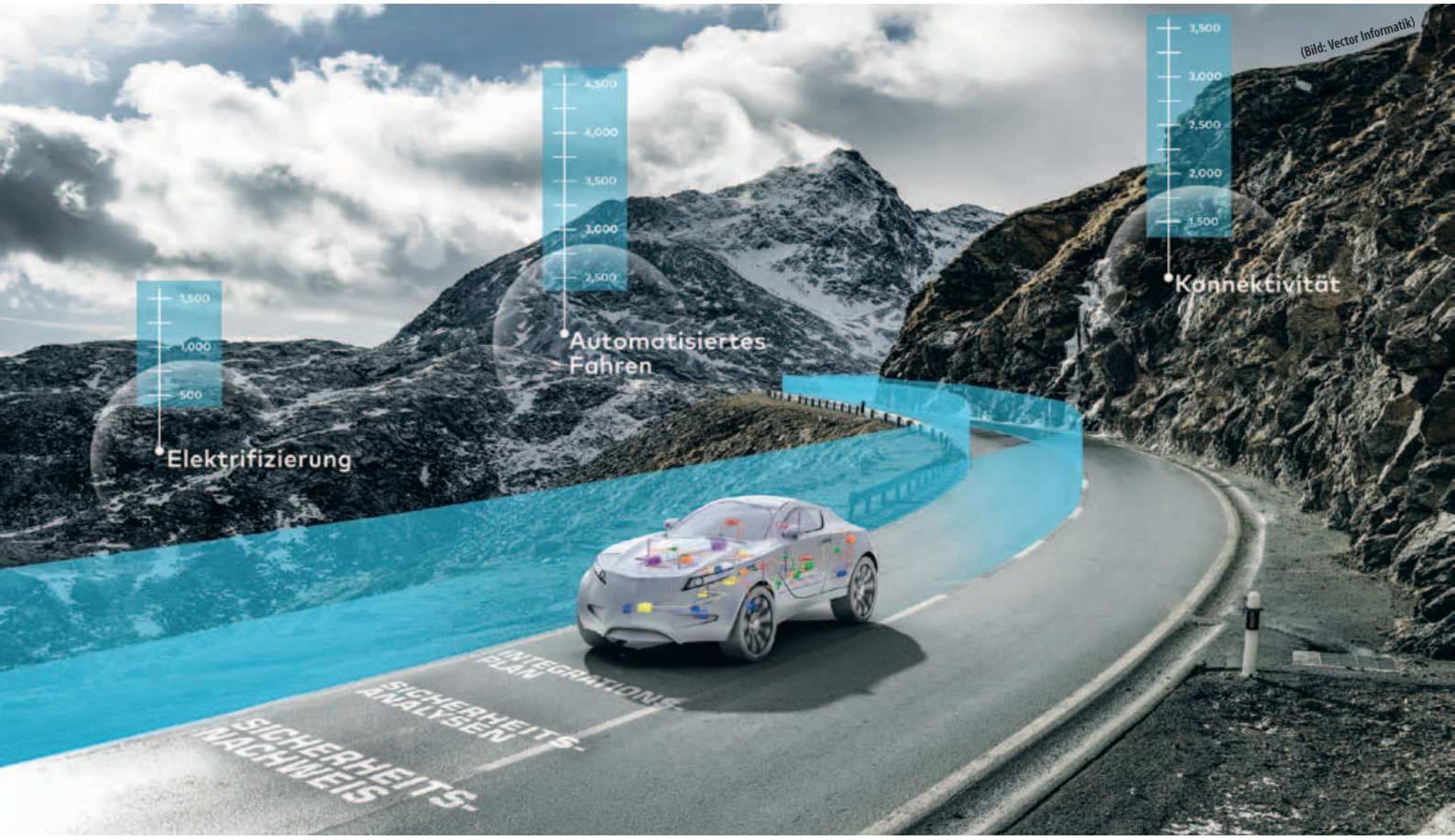

Modellbasierte E/E-Entwicklung konform zu ISO 26262:

Fortschrittliche Systeme – aber sicher!

Elektrifizierung, Automatisierung und Fahrzeugvernetzung stellen höchste Anforderungen an die funktionale Sicherheit von Fahrzeugen. Die elektronischen Systeme der neuen Fahrzeugfunktionen sind hochgradig vernetzt, was die Sicherheitsbetrachtung auf der Ebene des Gesamtsystems erforderlich macht. Zudem müssen auf technologischer Seite Trends wie Automotive Ethernet und AUTOSAR Adaptive berücksichtigt werden. Modellbasierte Entwicklungsumgebungen unterstützen Ingenieure dabei, beide Herausforderungen zu meistern.

Von Dr. Nico Adler

Bei der Elektrik/Elektronik-Entwicklung muss die funktionale Sicherheit auf allen Ebenen betrachtet werden. Dazu gehören das Architektur-Design, die Anforderungsanalyse, der Software- und Systementwurf, das Kommunikationsdesign sowie die Entwicklung der Hardware-Komponenten und des Leitungssatzes (**Bild 1**). Gleichzeitig ist die Wiederverwendung von Elektrik/Elektronik (E/E) in anderen Produktlinien und Ausstattungsvarianten zu berücksichtigen. Mit Hilfe konsistenter E/E-Modelle lassen sich einerseits die zahlreichen Optionen abbilden, die sich aufgrund dieser Freiheitgrade für die Entwicklung ergeben. Andererseits kann die Komplexität der Entwicklung funktional sicherer E/E-Systeme beherrscht werden.

ISO 26262 – ein Standard mit Zukunft

Die Vorgaben für die Entwicklung sicherheitsrelevanter E/E von Kraftfahrzeugen sind im Standard ISO 26262 international festgelegt. Er wurde im Pkw-Segment etabliert und kommt bereits in den Bereichen Zweiräder, Lkw, Busse, landwirtschaftliche Maschinen und auch bei Halbleiterherstellern zum Einsatz. Er stellt nicht nur umfas-

sende Anforderungen an die funktionale Sicherheit der Endprodukte, sondern auch an die Methoden und Prozesse der Produktentwicklung sowie an das Management. Bei der Standardisierung wurde auf bewährte Methoden der Sicherheitsanalyse und auf vorhandene Industriestandards zurückgegriffen. Aktuell wird eine Revision vorbereitet, die Erkenntnisse aus der Anwendung des Standards aufgreift und den Einsatzbereich ausweitet. Ein Werkzeug, mit dem sich die Vorgaben der ISO 26262 effizient umsetzen lassen, ist PREEvision. Vector stellt damit eine modellbasierte Lösung bereit, mit der alle Ebenen der E/E-Architektur eines Fahrzeugs in einer eigens dafür entwickelten Beschreibungssprache konsistent Werkzeug-gestützt abgebildet werden können. Mit ihr lässt sich die funktionale Sicherheit von E/E-Systemen und Komponenten analysieren und optimieren (**Bild 2**). Ausgehend von Anforderungen, die auf kundenspezifische, erlebbare Fahrzeugfunktionen bezogen werden können, wird die logische Systemarchitektur entworfen. Auf dieser lässt sich die Software- und Hardware-Architektur inklusive der Netzwerktopologie aufbauen. Außer der Systemsicht stellt das Werkzeug detaillierte Sichten auf die Schalt- und Stromlaufpläne sowie den Leitungssatz bereit. Ergänzend lassen sich die Layouts physikalischer Komponenten und Verbindungen sowie die Geometrie der Einbauräume im Fahrzeug hinterlegen. Ein Versions- und Änderungsmanagement unterstützt den Einsatz der Entwicklungsumgebung in Serienprojekten. Import- und Export-Schnittstellen, die zu relevanten Austauschformaten konform sind, integrieren PREEvision in die vorhandene Werkzeuglandschaft und Umgebung des Kunden.

Funktionales Sicherheitskonzept

Als Startpunkt für eine systematische Identifizierung von Fehlfunktionen der Fahrzeugfunktionen lässt sich die qualitative Analysemethode Hazard and Operability Study (HAZOP) einsetzen. Dazu werden Kundenfunktionen, Anforderungen oder logische Funktionen, die von der technischen Umsetzung in Software oder Hardware abstrahiert sind, herangezogen. Die HAZOP-Ergebnisse dienen als Basis für das „Hazard Analysis and Risk Assessment“ (HARA), bei dem die Sicherheitsziele festgelegt werden.

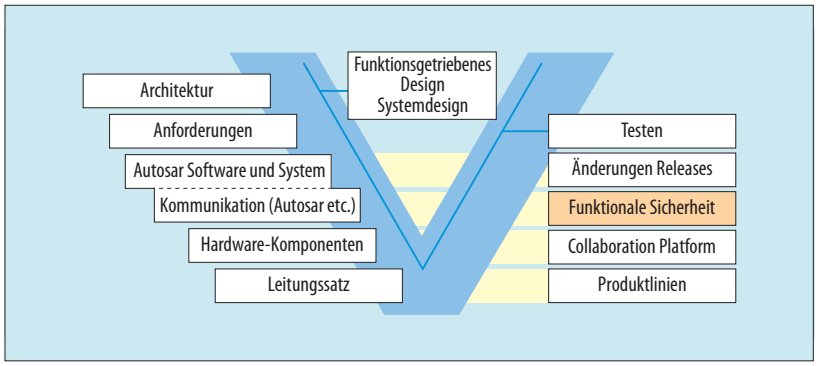

Bild 1. Funktionale Sicherheit ist ein integraler Bestandteil der E/E-Entwicklung. (Quelle: Vector Informatik)

Zum Festlegen der Gefährdungsereignisse (Hazardous Events) wird in PREEvision katalogbasiert sowohl auf Funktionen und zugehörige Fehlfunktionen als auch auf Betriebsmodi der Fahrzeugsysteme und Fahrsituationen zurückgegriffen. Durch Einstufen nach Schwere, Eintrittswahrscheinlichkeit und Beherrschbarkeit ergibt sich für jedes Gefährdungsereignis das Automotive Safety Integrity Level (ASIL). Auf dieser Grundlage werden die Sicherheitsziele mit zugehörigem ASIL festgelegt. Mit Hilfe Tabellen-basierter Editoren lassen sich ausgehend von den Sicherheitszielen funktionale Sicherheitsanforderungen spezifizieren. Durch Prüfungen des Modells, die das Werkzeug kontinuierlich im Hintergrund ausführt, werden Unzulässigkeiten wie invalide Dekompositionen von Sicherheitsanforderungen unmittelbar zurückgemeldet. Auf der logischen Architekturebene dienen Wirkketten zur Beschreibung des funktionalen Sicherheitskonzepts. Verwendet werden Sensor-, Aktuator und logische Funktionsblöcke, deren Ports durch Schnittstellendefinitionen spezifiziert sind. Eine Hierarchisierung logischer Funktionen ist ebenfalls möglich. Als Vorgehensweise hat sich das Beschreiben und Umsetzen einer Wirkkette pro Sicherheitsziel bewährt. Die Sicherheitsanforderungen lassen sich einfach mit den Objekten der logischen Ebene verknüpfen. So wird der Ingenieur bereits in der Konzeptphase in die Lage versetzt, die richtigen Maßnahmen zu treffen, um die Sicherheitsziele mit den zugehörigen ASIL zu erfüllen.

Technisches Sicherheitskonzept

Nach ISO 26262 werden im Rahmen der Produktentwicklung auf Systemebene die funktionalen zu technischen Sicherheitsanforderungen verfeinert und das Systemdesign sowie das technische Sicherheitskonzept erarbeitet. Das Referenz-Phasenmodell für die Entwicklung eines sicherheitsbezogenen Fahrzeugsystems sieht danach eine Aufteilung in die Produktentwicklung von Hardware und Software vor, die im Rahmen der Integration wieder auf Systemebene angehoben wird. Diesem Ansatz folgend bildet PREEvision das technische Sicherheitskonzept auf die Modellierungsebenen für Hardware und Software ab. Aus den technischen Sicherheitsanforderungen entstehen dabei spezifische Hardware- und Software-Sicherheitsanforderungen. Unterstützt durch Diagramme und Editoren lassen sich in PREEvision auf unterschiedlichen

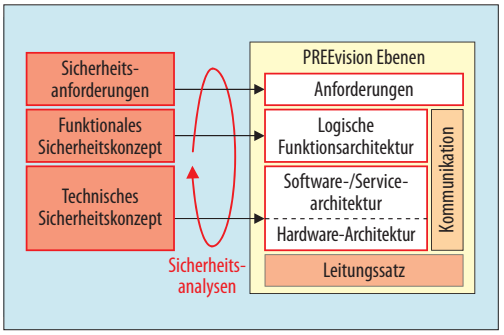

Bild 2. Das funktionale und technische Sicherheitskonzept wird in PREEvision auf den Ebenen logische Funktionsarchitektur, Software-/Servicearchitektur und Hardware-Architektur abgebildet. Die Sicherheitsanforderungen können mit entsprechenden Komponenten auf diesen Ebenen verknüpft werden. Durch werkzeuggestützte Sicherheitsanalysen kann das Sicherheitskonzept iterativ verfeinert und mit den Anforderungen in Einklang gebracht werden. (Quelle: Vector Informatik)

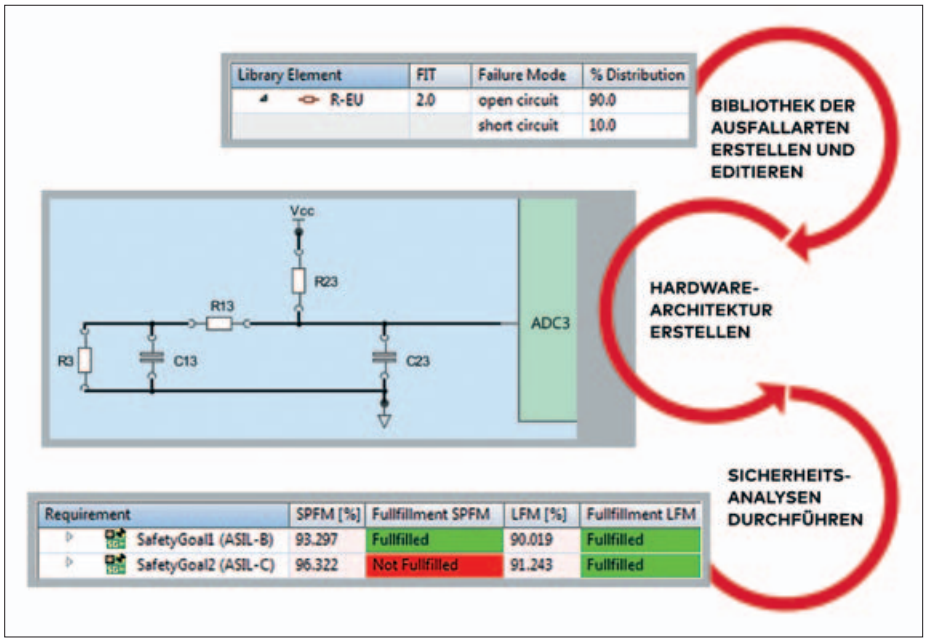

Bild 3. Sicherheitsanalysen für die Produktentwicklung auf Hardware-Ebene. (Bild: Vector Informatik)

Detailgraden arbeiten. So ist es möglich, sowohl das Architekturdesign als auch das detaillierte Design von Hardware- und Software-Komponenten zu erstellen. Dabei kommen Bibliotheken zum Einsatz, in denen die Ausfallrate und -arten für jedes Bauteil bereits hinterlegt sind. In ähnlicher Form können Sicherheitsmechanismen mit den zugehörigen Diagnoseabdeckungsgraden integriert werden (**Bild 3**).

Sicherheitsanalysen

Zur Sicherheitsanalyse der Designs unterstützt PREEvision die induktiven Methoden Failure Mode and Effects Analysis (FMEA), Failure Mode, Effects and Diagnostic Analysis (FMEDA) und die deduktive Fault-Tree-Analysis-Methode (FTA). Zum Durchführen einer FMEA lassen sich Formblätter mit Hilfe geeigneter Editoren manuell ausfüllen. Alternativ dazu kann PREEvision Anteile in einem FMEA-Formblatt auf Basis von Informationen aus dem Modell automatisch befüllen. Für die FTA kann der Anwender mit Hilfe von Diagrammen Fehlerbäume aufbauen und sie in Beziehung zu Sicherheitsanforderungen setzen. Das Ausführen einer qualitativen FTA ermittelt als Ergebnis Minimalschnitte, die zum Eintreten des untersuchten Hauptereignisses führen, zusammen mit den Wahrscheinlichkeiten für ihr Eintreten. Das bietet die Möglichkeit, die Designs gezielt zu verbessern. Zur Optimierung können im Diagramm zusätzlich relevante Designelemente aus dem Modell angezeigt werden. Um zu prüfen, ob die Designs die geforderten Zielwerte erreichen, kann eine quantitative FTA durchgeführt werden. Wie Teilsysteme lassen sich in PREEvision auch Fehlerbäume wiederverwenden. Im Kontext von Systemvarianten können Fehlerbäume variantensensitiv analysiert werden. Die FMEDA ist insbesondere für Tier-1 von Bedeutung. In PREEvision kann hierzu die Hardware bis auf die Ebene elektronischer Schaltpläne einer Komponente heruntergebrochen werden. Einzelne Bauteiltypen wie Mikrocontroller oder Widerstände werden in einer Bibliothek um Fehlerinformationen angereichert (Bild 3). Nach dem Instanziieren dieser Bauteile im Schaltplan kann der Ingenieur die einzelnen Ausfallarten der Bauteile in Bezug auf Einzel-, Rest- oder Mehrfachfehler einstufen. Darauf aufbauend lassen sich die geforderten Sicherheitsanalysen Hardware Architectural Metrics und Failure Rate Class Method durchführen. Durch die Integration aller notwendigen Informationen im PREEvision-Modell sind sowohl die Sicherheitsanforderungen, deren ASIL-Einstufung und die geforderten Zielwerte bekannt. Der Ingenieur erhält so eine direkte Rückmeldung darüber, ob diese erfüllt sind. Ein Ändern des Hardware-Designs kann zielgerichtet erfolgen, zum Beispiel durch Einführung von weiteren Sicherheitsmechanismen oder die Verwendung anderer Bauteile aus der Bibliothek.

Verifikation und Validierung

Zur Integration und zum Test auf Hardware-, Software- und Systemebene dient in PREEvision ein Testmanagement-Modul. Testspezifikationen können ausgehend von Anforderungen und Kundenfunktionen abgeleitet werden. Mit ihnen lassen sich die Tests entwerfen und implementieren. Es ist möglich, Testaktivitäten zu planen und die Ergebnisse der einzelnen Testausführungen – seien es manuelle Regressionstests oder automatisierte Tests – einzupflegen oder einzulesen. Die Ergebnisse bereitet das Werkzeug in Form von Berichten und Diagrammen auf.

Zusammenarbeit zwischen Automobilherstellern und -zulieferern

Durch ein Änderungsmanagement mit Ticketsystem können Änderungsanfragen und Defekte transparent verfolgt werden, indem sich Tickets mit Modellelementen verknüpfen lassen. Zusätzlich lassen sich kundenspezifische Lebenszyklen für Tickets festlegen. Ein integriertes Release-Management unterstützt die Projektplanung und -verfolgung. Darüber hinaus ist ein Review aller Modellanteile beispielsweise von Sicherheitsanforderungen möglich. Mit Hilfe einer Import-/Export-Schnittstelle, die das etablierte ReqIF-Austauschfor-

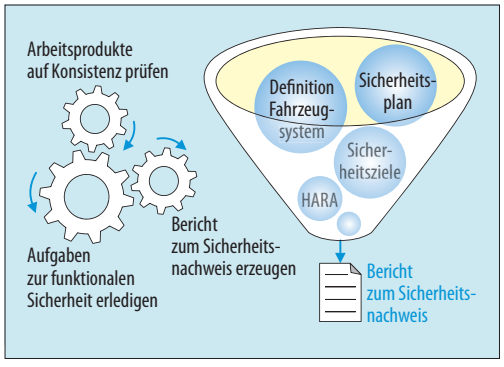

Bild 4. Sicherheitsnachweis als inkrementelle Aktivität. (Quelle: Vector Informatik)

mat erweitert, kann gleichzeitig eine externe Abstimmung von Anforderungen zwischen OEM und mehreren Lieferanten initiiert werden. Dieser Mechanismus unterstützt das in ISO 26262 erwähnte Development Interface Agreement für den Datenaustausch.

Iterativ zum Sicherheitsnachweis

Die von ISO 26262 geforderten Nachweisdokumente können mit einer individuell anpassbaren Reportgenerierung automatisch erstellt werden. In den Texten der Nachweisdokumente lassen sich Hyperlinks zum E/E-Modell hinterlegen. Das vereinfacht interne Reviews, Safety-Assessments und Audits. ISO 26262 empfiehlt, den Sicherheitsnachweis nicht erst gegen Ende des Sicherheitslebenszyklus anzugehen, sondern als inkrementelle Aktivität zu behandeln. Mit PREEvision kann der Ingenieur Entwicklungsaufgaben im Rahmen der funktionalen Sicherheit deshalb iterativ bearbeiten. Während unterschiedlicher Entwicklungsphasen können Arbeitsprodukte auf Konsistenz geprüft und ein Zwischenbericht zum Sicherheitsnachweis generiert werden. Diese Vorgehensweise führt am Schluss zum Sicherheitsnachweis, der belegt, dass alle Sicherheitsziele vollständig und erfüllt sind (**Bild 4**).

Modellbasierte Entwicklung

Modellbasierte Umgebungen bieten unterschiedliche Sichten auf die Fahrzeug-E/E und stellen ein leistungsfähiges Mittel für die Entwicklung dar. Sie ermöglichen einen konsistenten Entwurf funktional sicherer Systeme und helfen Ingenieuren dabei, sich auf den Kern ihrer Arbeit zu fokussieren. Leistungsfähige Werkzeuge wie PREEvision bieten darüber hinaus eine Prozessunterstützung, die sich an den Bedarf von OEM und Tier-1 anpassen lässt. Eine Nachverfolgbarkeit von der Anforderungsspezifikation bis hin zum Sicherheitsnachweis ist durch den integrierten Ansatz gegeben. *eck*

Dr. Nico Adler
arbeitet als Produktmanager „PREEvision Funktionale Sicherheit" bei Vector Informatik.

Lauterbach GmbH
Altlaufstraße 40
D 85635 Höhenkirchen
Tel. +49 8102 9876 - 0
Fax +49 8102 9876 - 187
sales@lauterbach.com
www.lauterbach.com

Highlights
Unter der Marke TRACE32 stehen dem Kunden sämtliche Lösungen für Debugging, Real-Time Trace und Logik-Analyse im Bereich Embedded Designs mit der größten Abdeckung von 16- bis 64-bit Prozessoren zur Verfügung. Die Produktlinie unterstützt JTAG, SWD, NEXUS oder ETM für mehr als 3500 Cores und CPUs verschiedener Familien wie Arm Cortex-A/-M/-R, PowerArchitecture, TriCore, RH850, MIPS etc.

Firmenprofil
- Gründungsjahr: 1979
- Mitarbeiter: 120

Zielmärkte
- Automotive
- Communication
- Industry
- Aerospace
- Medical

Firmenausrichtung
Technologieführer von modularen Mikroprozessor-Entwicklungswerkzeugen

Produkte/Linecard
Debugger
Trace Systeme

Standorte/Lager
Höhenkirchen b. München
Italien, Frankreich, USA, UK, China, Japan, Tunesien

Qualitätsmanagement
ISO 9001

SCHEID automotive GmbH
Werner-von-Siemens-Straße 2-6
D 76646 Bruchsal
Tel. +49 7251 936991-0
info@scheid-automotive.com
www.scheid-automotive.com

Highlights
Software-Entwicklung basierend auf AUTOSAR.

Firmenprofil
- Gründungsjahr 2011

Firmenausrichtung
SCHEID automotive GmbH ist eine Software-Engineering-Firma in Bruchsal. Wir planen, organisieren und führen Software-Entwicklungsprojekte für Automotive-Anwendungen auf der Basis von AUTOSAR aus.
Wir sind seit 2017 AUTOSAR Associate Member.

Produkte/Linecard
AUTOSAR-Software-Components, Complex Driver, Libraries

Dienstleistungen/Service
Konfiguration, Integration, Entwicklung und Portierung von AUTOSAR-Systemen